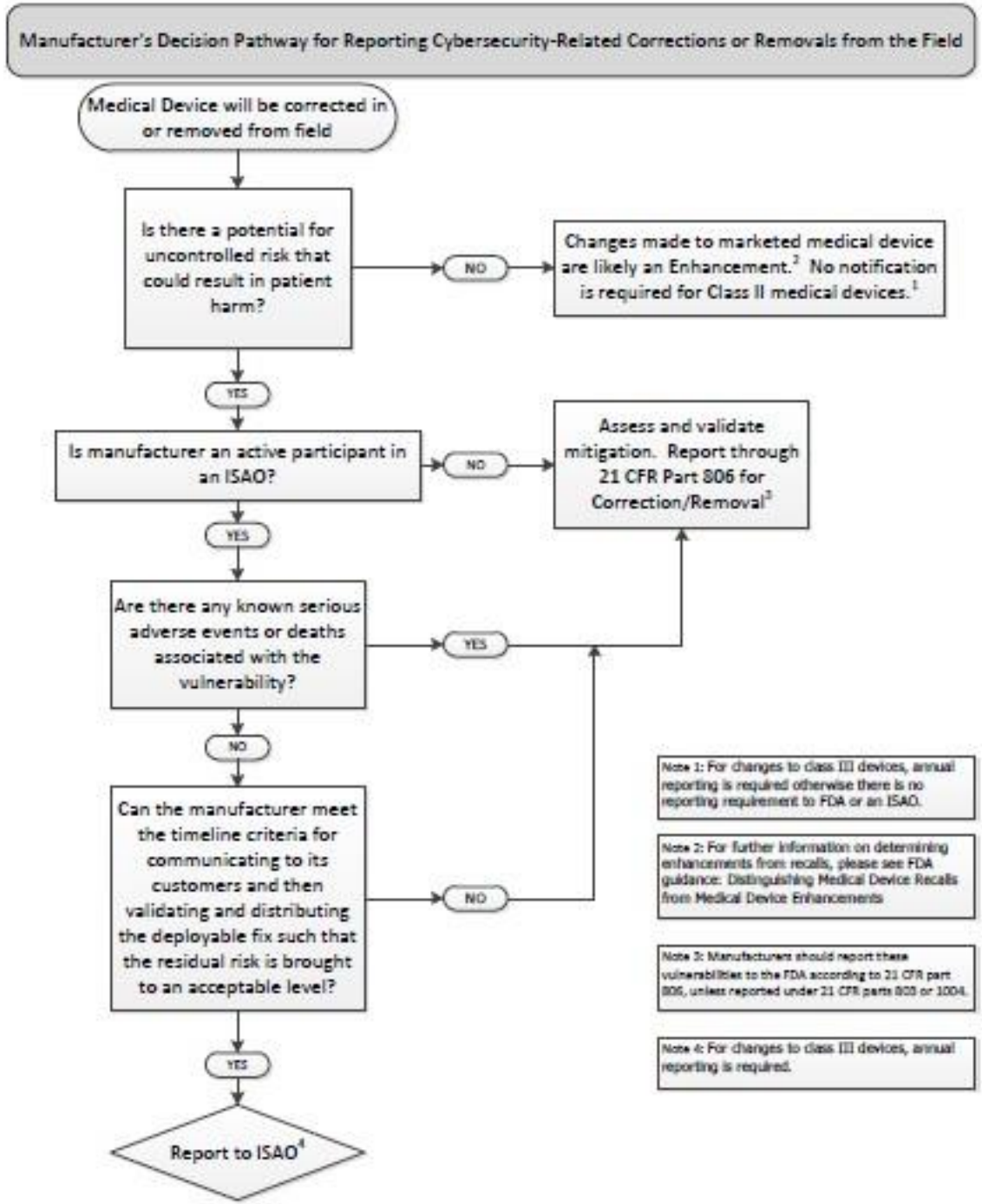

Manufacturer's Decision Pathway for Reporting Cybersecurity-Related Corrections or Removals from the Field
Medical Device will be corrected in or removed from field
Is there a potential for uncontrolled risk that could result in patient harm?
NO
Changes made to marketed medical device are likely an Enhancement.[2] No notification is required for Class II medical devices.[1]
YES
Is manufacturer an active participant in an ISAO?
NO
Assess and validate mitigation. Report through 21 CFR Part 806 for Correction/Removal[3]
YES
Are there any known serious adverse events or deaths associated with the vulnerability?
YES
NO
Can the manufacturer meet the timeline criteria for communicating to its customers and then validating and distributing the deployable fix such that the residual risk is brought to an acceptable level?
NO
YES
Report to ISAO[4]
Note 1: For changes to class III devices, annual reporting is required otherwise there is no reporting requirement to FDA or an ISAO.
Note 2: For further information on determining enhancements from recalls, please see FDA guidance: Distinguishing Medical Device Recalls from Medical Device Enhancements
Note 3: Manufacturers should report these vulnerabilities to the FDA according to 21 CFR part 806, unless reported under 21 CFR parts 803 or 1004.
Note 4: For changes to class III devices, annual reporting is required.

MD-VIPER

Medical Device Vulnerability Sharing

Stakeholders

including manufacturers, healthcare delivery organizations (HDOs), independent security researchers, regulatory agencies, etc.

Benefits – Sharing of

- ❑ reports on known vulnerabilities
- ❑ vetting and evaluation of vulnerabilities
- ❑ details of actions taken by others to mitigate vulnerabilities
- ❑ medical device cybersecurity education, best practices, mitigation strategies

MD-VIPER

MD-VIPER Vulnerability Report for Manufacturers

The *MD-VIPER Vulnerability Report* is designed to serve as an alternate reporting process to FDA's requirements for *21 CFR Part 806* reporting if cybersecurity vulnerabilities are involved.

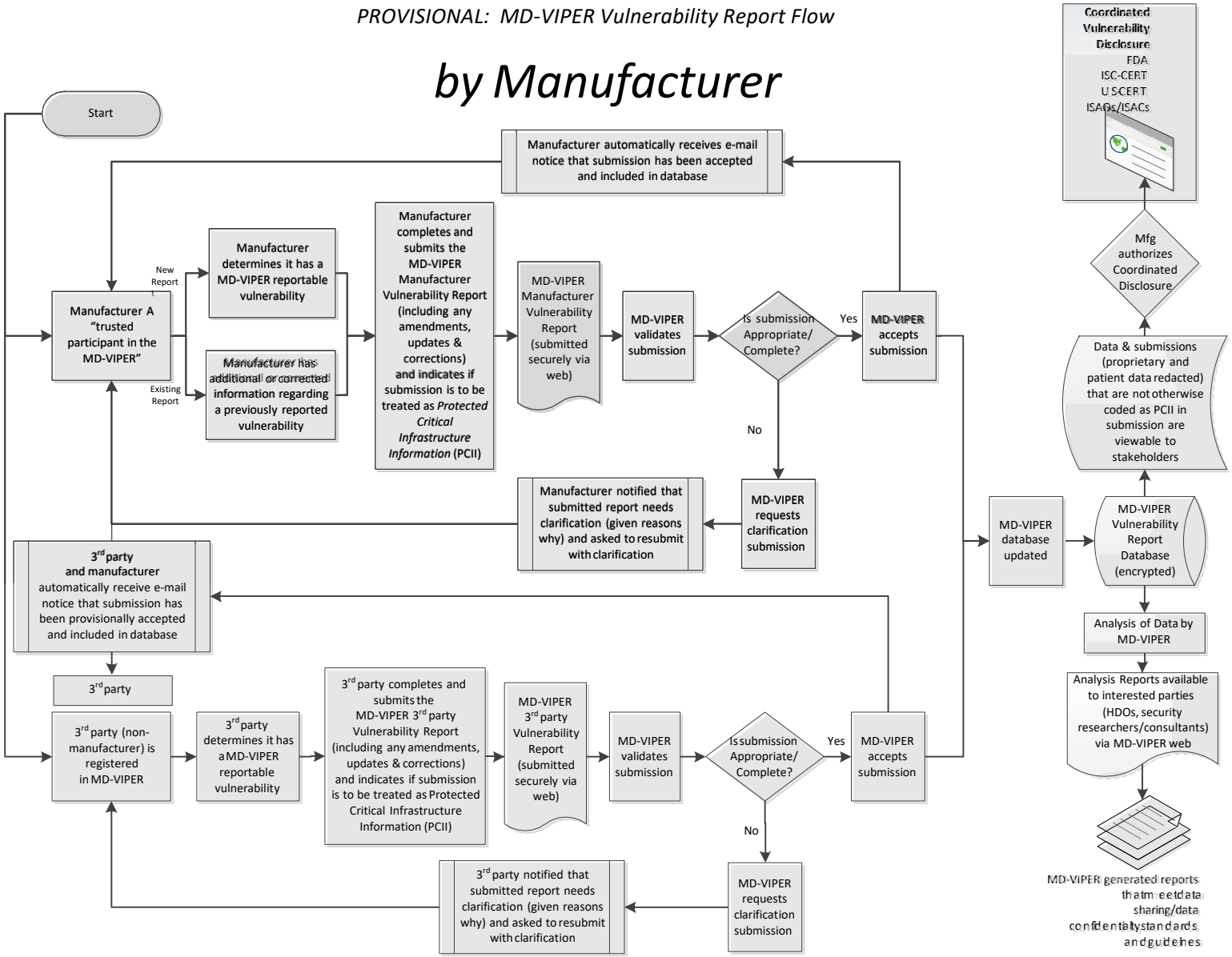
Manufacturers are not held to *21 CFR Part 806* reporting requirements if

- ❑ the manufacturer is a active participant in an ISAO (such as NH-ISAC)
- ❑ the manufacturer is conducting a correction/removal to address a cybersecurity vulnerability
- ❑ the cybersecurity vulnerability in question has not led to any known serious injuries or deaths
- ❑ the manufacturer will meet the timeline criteria for communicating to its customers and then validating and distributing the deployable fix such that the residual risk is brought to an acceptable level

Medical Device Vulnerability Reporting Workflow

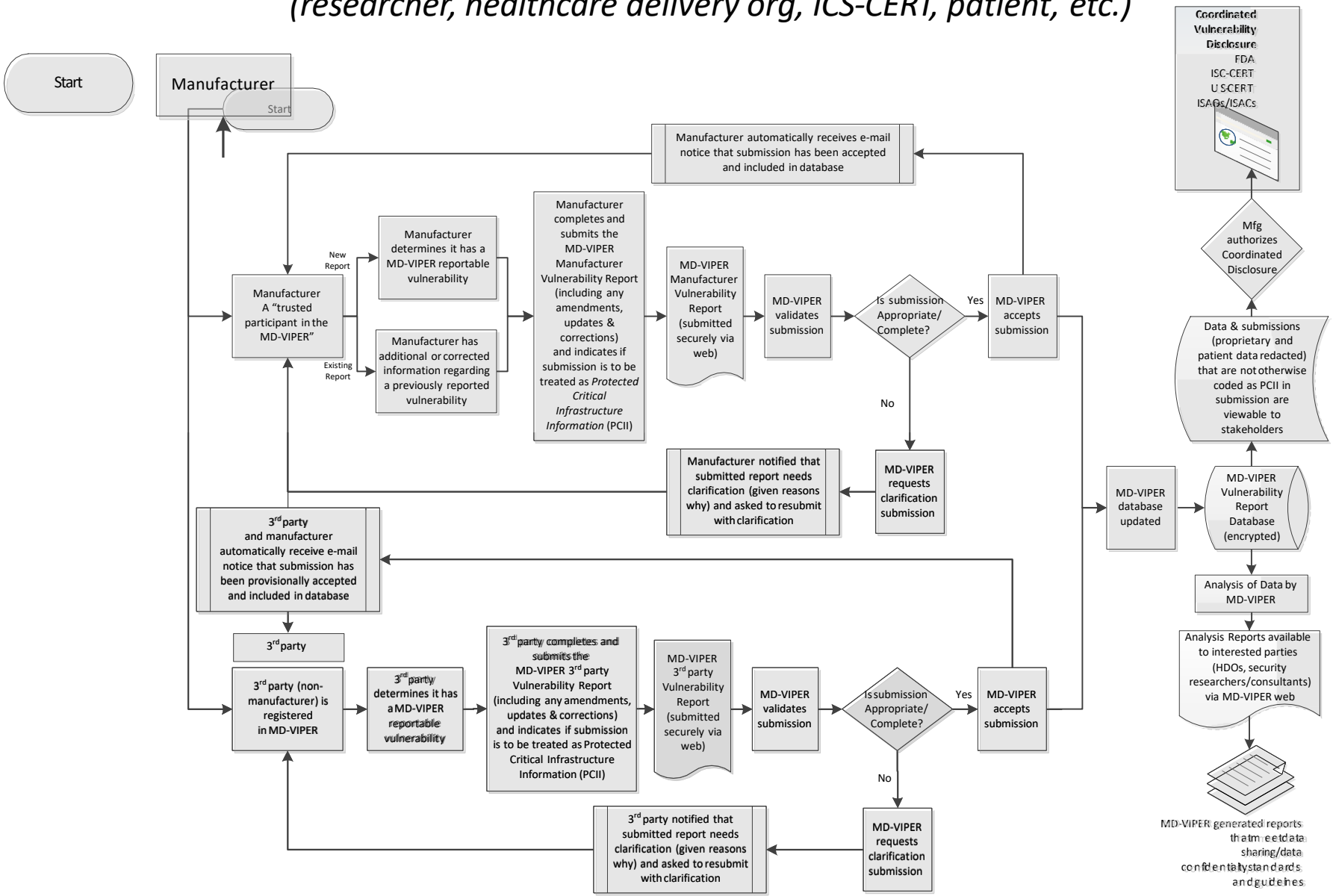
PROVISIONAL: MD-VIPER Vulnerability Report Flow

by Manufacturer

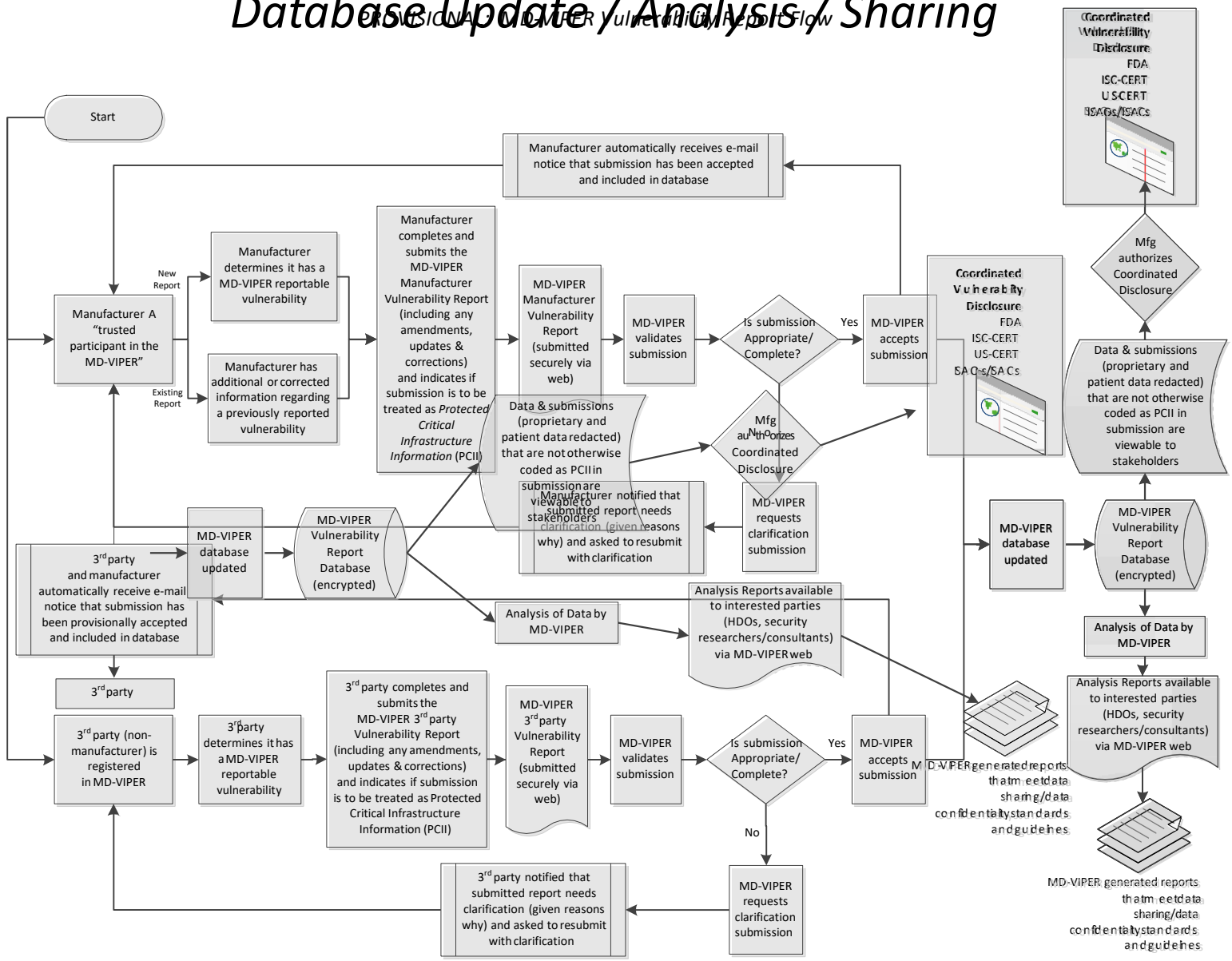


Medical Device Vulnerability Reporting Workflow by Non-manufacturer

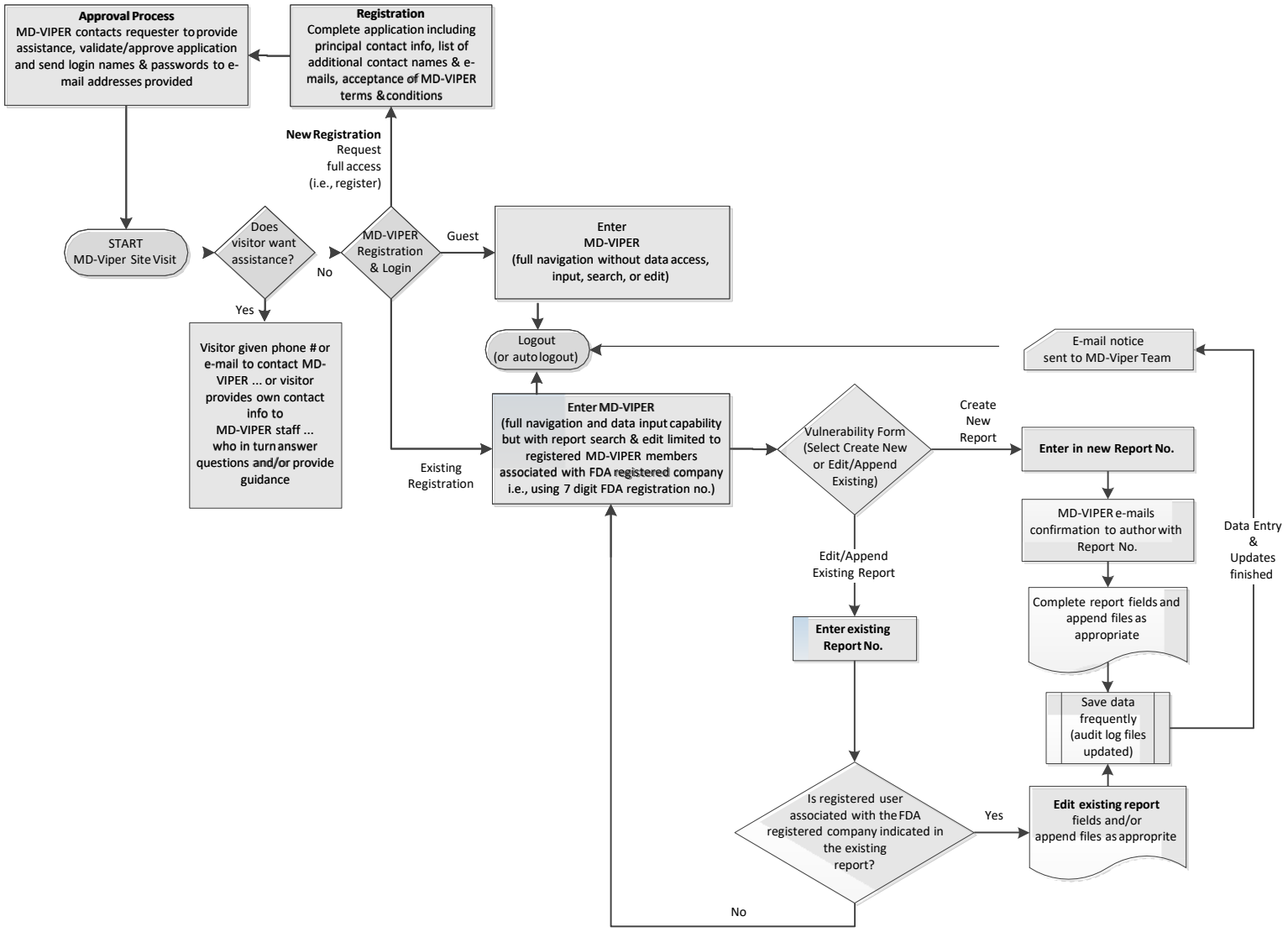
(researcher, healthcare delivery org, ICS-CERT, patient, etc.)



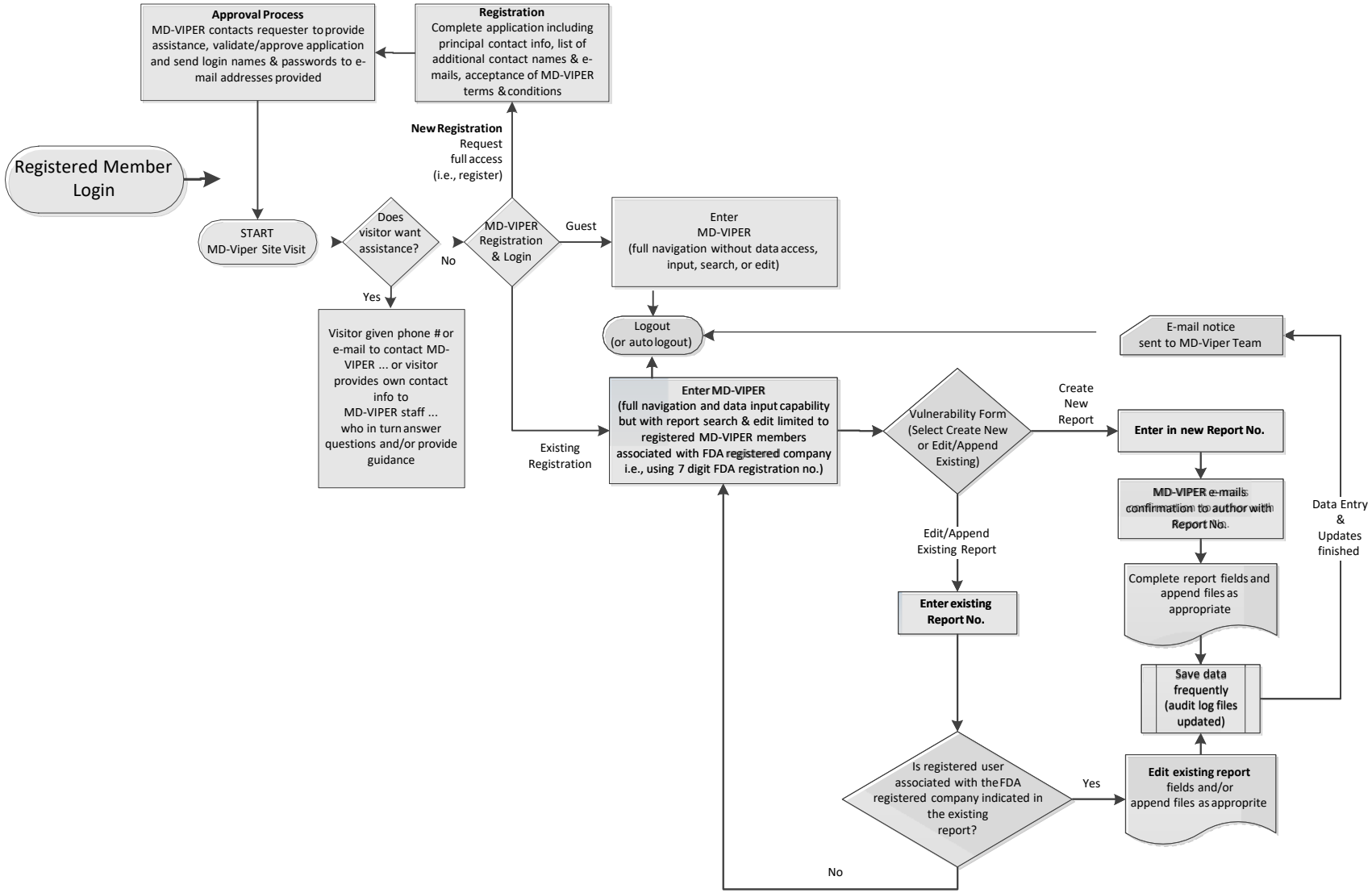
Medical Device Vulnerability Reporting Workflow Database Update / Analysis / Sharing



MD-VIPER Site Access



MD-VIPER Site Access – Member Create / Modify Reports



MD-VIPER

MD-VIPER Vulnerability Report for Manufacturers

The *MD-VIPER Vulnerability Report* is designed to serve as an alternate reporting process to FDA's requirements for 21 CFR Part 806 reporting if cybersecurity vulnerabilities are involved.

- ❑ **Questions 1-6 and 8-13** on the MD-VIPER report closely map to the questions in Part 806 reports
- ❑ **Question 7** on the FDA's 806 report asks for a description of events leading the report and any actions taken while question 7 on the MD-VIPER report asks for details about the cybersecurity aspects of the vulnerability
- ❑ **Question 14** has been added to the MD-VIPER report to request that those responses to report questions containing information that could be exploited be treated as *Protected Critical Infrastructure Information* and therefore kept confidential

MD-VIPER Vulnerability Report for Manufacturers

1. Report Number ..... [ ] 806
   (includes 7 Digit Manufacturer Registration No.)
2. Manufacturer (or Importer)
   Company Name ..... [ ] 806
   Street Address ..... [ ] 806
   City, State Zip ..... [ ], [ ] [ ] 806
   Contact Name (*Last, First*) ..... [ ] 806
   Phone ..... [ ] 806
   e-mail ..... [ ] 806
3. FDA Classification name of the device ..... [ ] 806
4. Marketing status of the device ..... [ ] 806
   (i.e., 510(k), PMA #, preamendment status &
   device listing number)
5. Unique Device Identifier (UDI) ..... [ ] 806
   (or model/catalog number, lot/serial number)
6. Manufacturer (if different from #2)
   Company Name ..... [ ] 806
   Street Address ..... [ ] 806
   City, State Zip ..... [ ], [ ] [ ] 806
   Phone ..... [ ], [ ] [ ] 806